

1 CLAIMS

2 What is claimed is:

3 1. A method of processing messages, comprising:

4 comparing a nonce value of a received message with a largest nonce value yet
5 seen;

6 comparing said nonce value to an acceptance window in response to said
7 nonce value not exceeding said largest nonce value yet seen; and

8 rejecting said received message in response to said nonce value falling outside
9 said acceptance window.

10
11 2. The method according to claim 1, further comprising:

12 designating said nonce value as a nonce value seen in response to said nonce
13 value exceeding said largest nonce value yet seen.

14
15 3. The method according to claim 1, further comprising:

16 replacing said largest nonce value yet seen with said nonce value in response
17 to said nonce value exceeding said largest nonce value yet seen.

18
19 4. The method according to claim 1, further comprising:

20 adjusting an acceptance window based on said nonce value in response to said
21 nonce value exceeding said largest nonce value yet seen.

22

1 5. The method according to claim 1, further comprising

2 designating said received message as a replay attack.

3
4 6. The method according to claim 1, further comprising:

5 comparing said nonce value to a window mask value in response to said nonce

6 value falling within said acceptance window; and

7 rejecting said received message in response to an outcome of said comparison

8 of said nonce value to said window mask value being true.

9
10 7. The method according to claim 6, further comprising:

11 designating said received message as part of a replay attack.

12
13 8. The method according to claim 1, further comprising:

14 comparing said nonce value to a window mask value in response to said nonce

15 value falling within said acceptance window; and

16 accepting said received message in response to an outcome of said comparison

17 of said nonce value to said window mask value being false.

18
19 9. The method according to claim 8, further comprising:

20 designating said nonce value as a nonce value seen.

21
22 10. An apparatus for processing messages, said apparatus comprising:

1 a communication interface configured to transmit and receive a plurality of
2 packets; and

3 a controller, wherein said controller is configured to:

4 compare a nonce value of a received message and a largest nonce value
5 yet seen;

6 compare said nonce value to an acceptance window in response to said
7 nonce value not exceeding said largest nonce value yet seen; and

8 reject said received message in response to said nonce value falling
9 outside said acceptance window.

10
11 11. The apparatus according to claim 10, wherein said controller is further
12 configured to designate said nonce value as said largest nonce value yet seen in response to
13 said nonce value exceeding said largest nonce value yet seen.

14
15 12. The apparatus according to claim 10, wherein said controller is further
16 configured to adjust an acceptance window in response to said largest nonce value yet seen in
17 response to said nonce value exceeding said largest nonce value yet seen.

18
19 13. The apparatus according to claim 10, wherein said controller is further
20 configured to replace said largest nonce value yet seen with said nonce value in response to
21 said nonce value exceeding said largest nonce value yet seen.

1 14. The apparatus according to claim 10, wherein said controller is further
2 configured to designate said received message as part of a replay attack.

3
4 15. The apparatus according to claim 10, wherein said controller is further
5 configured to:

6 compare said nonce value to a window mask value in response to said
7 nonce value falling within said acceptance window; and

8 reject said received message in response to an outcome of said
9 comparison of said nonce value to said window mask value being true.

10
11 16. The apparatus according to claim 15, wherein said controller is further
12 configured to designate said received message as part of a replay attack

13
14 17. The apparatus according to claim 10, wherein said controller is
15 configured to:

16 compare said nonce value to a window mask value in response to said
17 nonce value falling within said acceptance window; and

18 accept said received message in response to an outcome of said
19 comparing of said nonce value to said window mask value being false.

20
21 18. The apparatus according to claim 17, wherein said controller is further
22 configured to mark said nonce value as a nonce value seen.

1 19. A computer readable storage medium on which is embedded one or
2 more computer programs, said one or more computer programs implementing a method of
3 processing messages, said one or more computer programs comprising a set of instructions
4 for:

5 comparing a nonce value of a received message and a largest nonce value yet
6 seen;

7 comparing said nonce value to an acceptance window in response to said
8 nonce value not exceeding said largest nonce value yet seen; and

9 rejecting said received message in response to said nonce value not falling
10 within said acceptance window.

11
12 20. The computer readable storage medium in according to claim 19, said
13 one or more computer programs further comprising a set of instructions for:

14 designating said nonce value as a nonce value seen in response to said nonce
15 value exceeding said largest nonce value yet seen..

16
17 21. The computer readable storage medium in according to claim 19, said
18 one or more computer programs further comprising a set of instructions for:

19 replacing said largest nonce value yet seen with said nonce value in response
20 to said nonce value exceeding said largest nonce value yet seen.

1 22. The computer readable storage medium in according to claim 19, said
2 one or more computer programs further comprising a set of instructions for:
3 adjusting an acceptance window based on said nonce value in response to said
4 nonce value exceeding said largest nonce value yet seen.

5
6 23. The computer readable storage medium in according to claim 19, said
7 one or more computer programs further comprising a set of instructions for:
8 designating said received message as a replay attack.

9
10 24. The computer readable storage medium in according to claim 19, said
11 one or more computer programs further comprising a set of instructions for:
12 comparing said nonce value to a window mask value in response to said nonce
13 value falling within said acceptance window; and
14 rejecting said received message in response to an outcome of said comparison
15 of said nonce value to said window mask value being true.

16
17 25. The computer readable storage medium in according to claim 24, said
18 one or more computer programs further comprising a set of instructions for:
19 designating said received message as part of a replay attack.

20
21 26. The computer readable storage medium in according to claim 19, said
22 one or more computer programs further comprising a set of instructions for:

1 comparing said nonce value to a window mask value in response to said nonce
2 value falling within said acceptance window; and
3 accepting said received message in response to an outcome of said comparing
4 of said nonce value to said window mask value being false.

5

6 27. The computer readable storage medium in according to claim 26, said
7 one or more computer programs further comprising a set of instructions for:
8 designating said nonce value as a nonce value seen.

9

10

11

12

13

14

15

16

17

18

19

20

21

28. A system for processing messages in a peer-to-peer configuration,
comprising:

a first peer configured to provide secure communication;

a second peer configured to provide said secure communication; and

a secure communication module configured to be executed by said first peer

and second peer, wherein said secure communication module is configured to:

compare said nonce value to a filter in response to a nonce value of a
received packet not exceeding a largest nonce value yet seen;

compare said nonce value to a replay mask; and

accept said received packet in response to said comparison of said
nonce value and said replay mask being false.

1 29. The system according to claim 28, wherein said secure communication
2 module is further configured to designate said nonce value as said largest nonce value yet
3 seen in response to said nonce value exceeding said largest nonce value yet seen.

4

5 30. The system according to claim 28, wherein said secure communication
6 module is further configured to adjust said filter based on said largest nonce value yet seen in
7 response to said nonce value exceeding said largest nonce value yet seen.

8

9 31. The system according to claim 28, wherein said secure communication
10 module is further configured to reject said received packet in response to said nonce value
11 falling outside said filter.

12

13 32. The system according to claim 31, wherein said secure communication
14 module is further configured to designate said received packet as part of a replay attack.

15

16 33. The system according to claim 32, wherein said secure communication
17 module is further configured to reject said received packet in response to said comparison of
18 said nonce value and said replay mask being true.

19

20 34. The system according to claim 33, wherein said secure communication
21 module is further configured to designate said received packet as part of a replay attack.

22

1 35. The system according to claim 28, wherein said secure communication
2 module is further configured to reject said received packet in response to said nonce value
3 fails to fall within said filter and said secure communication module is further configured to
4 designate said received packet as part of a replay attack.

5

6 36. An interceptor device for processing messages, said interceptor device
7 comprising:

8 a network interface;

9 an expected sequence register configured to enumerate an expected sequence
10 number of a packet received from a second network device;

11 a memory configured to store a replay mask; and

12 a controller, wherein said controller is configured to:

13 compare said nonce value to a filter in response to a sequence number
14 of a received packet via said network interface does not exceed a largest sequence number yet
15 seen retrieved from said expected sequence register;

16 compare said sequence number to said replay mask retrieved from said
17 memory; and

18 accept said received packet in response to said comparison of said
19 sequence number and said replay mask is false.

20

1 37. The interceptor device according to claim 36, wherein said controller is
2 further configured to designate said sequence number as said largest sequence number yet
3 seen in response to said sequence number exceeding said largest sequence number yet seen.
4

5 38. The interceptor device according to claim 36, wherein said controller is
6 further configured to adjust said filter based on said largest sequence number yet seen in
7 response to said sequence number exceeding said largest sequence number yet seen.
8

9 39. The interceptor device according to claim 36, wherein said controller is
10 further configured to reject said received packet in response to said sequence number falling
11 outside said filter.
12

13 40. The interceptor device according to claim 36, wherein said controller is
14 further configured to designate said received packet as part of a replay attack.
15

16 41. The interceptor device according to claim 36, wherein said controller is
17 further configured to reject said received packet in response to said comparison of said
18 sequence number and said replay mask being true.
19

20 42. The interceptor device according to claim 41, wherein said controller is
21 further configured to designate said received packet as part of a replay attack.
22

